An IoT and Blockchain-based Approach for Ensuring Transparency and Accountability in Regulatory Compliance

Conference or Workshop Item

An IoT and Blockchain-based Approach for Ensuring Transparency and Accountability in Regulatory Compliance

Niaz Chowdhury
niaz.chowdhury@open.ac.uk
The Open University
United Kingdom

ABSTRACT

Regulatory compliance is an essential exercise in the modern societies confirming safety and prevention of harm to consumers. Despite many efforts from international and national quality control authorities, transparency and accountability in regulatory compliance remain a challenging technical-legal problem sitting atop a heavy reliance on trust. This paper presents a theoretical model of regulatory compliance aiming at improving accountability for systems and data audit and introduces a higher degree of transparency in management and quality control. It explores the technical aspects of two emerging technologies the Internet of Things (IoT) and Blockchain, and using a common use-case in practice shows how to better align these technologies with legal concerns and trust in regulatory compliance.

CCS CONCEPTS

• **General and reference** → *Surveys and overviews.*

KEYWORDS

regulatory compliance, internet of things, blockchain, trust

ACM Reference Format:
Niaz Chowdhury. 2019. An IoT and Blockchain-based Approach for Ensuring Transparency and Accountability in Regulatory Compliance. In *Proceedings of UbiComp/ISWC '19 Adjunct, September 9–13, 2019, London, United Kingdom.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

UbiComp/ISWC '19 Adjunct, September 9–13, 2019, London, United Kingdom,
,

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM.
https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

The regulatory compliance is the adherence to laws, regulations, guidelines and specifications relevant to the business of a firm involved. It shows the firms' aspiration in ensuring what the regulation asked to comply with and is an essential exercise in the modern societies confirming safety and prevention of harm to consumers [5, 10]. International organisations such as the World Health Organization (WHO) and the International Organization for Standardisation (ISO) have been working toward producing guidelines for the firms for many decades. Numerous regional and national organisations have also been involved in applying local quality controls within their jurisdiction.

Despite all these efforts from international and local organisations, transparency and accountability in regulatory compliance remain a challenging technical-legal problem sitting atop a heavy reliance on trust. The current practice accounts for moral obligation and social influence where quality controlling authorities primarily focuses on the certainty and severity of sanctions as key determinants. However, they do not consider all possible tangible and intangible motivations that influence firms' decision to comply with a particular set of guidelines. Furthermore, their investigative methods comprising surprise inspection and scrutinising records may not always result in finding the oddity in firms' operational behaviour due to having enough loopholes in the recordkeeping techniques and the lack of use of appropriate technologies. Therefore, despite living in the era of technological innovation, still, trust plays a vital role in regulatory compliance and often the process works based on the assumption that all parties would cooperate unconditionally.

This paper presents a theoretical model of technology-backed regulatory compliance to establish more transparency and accountability in the process. In doing so, it uses a food safety use-case and two disruptive technologies made available to the public recently. The paper argues that the use of IoT and Blockchain technology can effectively remove the need for trust in regulatory compliance giving both quality control authorities and firms access to immutable data to enhance their participation in the process. That said, it is

not the intention of the author to indicate that the participating firms in the existing practice always try to hide their oversights or quality control authorise are inadequate. The proposed model aims to overcome the existing shortcomings and introduces new perspectives in the monitoring process. While this model is discussed in a food safety context, the approach developed here applies to a variety of other use-cases from a wide range of industries.

The contribution of the paper is in twofold: First, it identifies the loopholes in the existing practice of the used use-case and second, it presents a theoretical model of regulatory compliance for the use-case replacing the need for trust by an IoT and Blockchain-based technological architecture.

2 FOOD SAFETY USE-CASE: TEMPERATURE CONTROL

The theoretical model of regulatory compliance presented in this paper is developed in the context of food safety in the United Kingdom (UK) and mainly focusing on the temperature regulation associated with the refrigerators at restaurants and bakeries (hereafter used synonymously) in the country.

The Food Safety (Temperature Control) Regulations 1995 states that the temperature inside the refrigerators at the restaurants and bakeries must be kept at or below 8°C [1, 7]. The temperature range of above 8°C and below 63°C is commonly known as the *Danger Zone* for microbial growth. When the temperature moves over this threshold, the likelihood of having bacteria in the food is very high, and therefore, restaurants and bakeries must comply with this regulatory temperature of below 8°C in their refrigerators at all time. Due to avoiding the potential risk of creating a health hazard and a subsequent fine, some local government authorities in the UK suggest even a lower threshold of 5°C. There are no defined temperatures for freezers, but most local authorities recommend a temperature of -18°C or below [12].

As a part of the food safety regulatory compliance, restaurants are obliged to measure the temperature of each refrigerator used in storing and serving food four times a day if they remain open 24 hours or just twice for the day restaurants. The measured temperature needs to be noted down somewhere securely, and the records must be made available upon request by the authorities, particularly at the time of the inspection. During the measurement, if a refrigerator is found having a temperature of more than 8°C threshold, restaurants must investigate the incident and come up with a report stating the cause of the temperature hike and necessary steps taken by the manager to mitigate the risks. Food inspectors during their visit read these reports and examine if the due diligence were adequately performed or a sanction is necessary.

Figure 1: Refrigerators used in the restaurants can be of different types and sizes. The above images show a display fridge (top) commonly seen at the bakeries in the UK, a small fridge (middle) and a large freezer (bottom) from the backroom of a restaurant.

The use-case shows the need for three tasks: i) Scheduling temperature measurement, ii) Measuring the temperature, and ii) Keeping records of the measurement and making it available to the inspector at the time of inspection or investigation. This study looks at these three tasks and explore how these tasks are currently being performed, what are the potential loopholes in the practice and finally propose our conceptual model to mitigate the loopholes and establish more transparency and accountability in performing these tasks.

3 CURRENT PRACTICE AND PROBLEMS

In this study, the author took a field survey approach and visited several restaurants located in the England region of the UK. During the visits, the author talked to the managers in a bid to understand their regulatory compliance with the necessary temperature management. What the author learned from the discussions is quite remarkable. Although there exists a clearly defined specification for the temperature to be maintained in the refrigerators, no defined guideline as to how to manage the records is available. Restaurants do it in various ways. The most common practice being the use of paper-based record maintenance. For example, figure 2 shows a copy of a recordkeeping form from a restaurant located in Milton Keynes. Some of the restaurants also use smartphone and tablet applications to input and store the records. The author had come across one such company, *Akeman Solutions*, who develop and sell customised smartphone application built only for keeping records of temperature in the restaurants. Figure 3 shows a screenshot of the application from one of the restaurants they provide this service with.

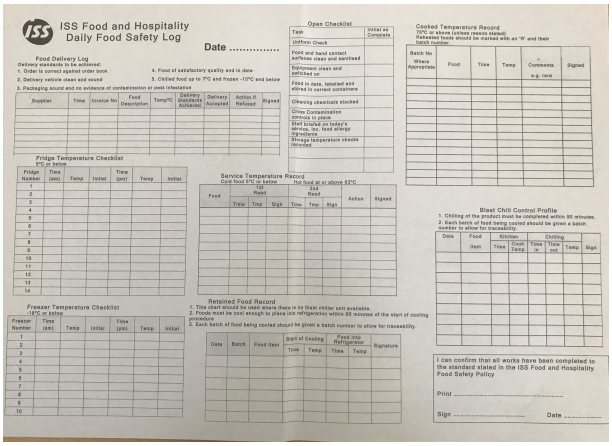

Figure 2: Daily food safety log showing tables for recording temperature from a verity of refrigerators from a local restaurant in England, UK.

The author observed that these records are maintained based on trust, and there remains a common assumption that all parties would cooperate unconditionally. While the author does not indicate that everyone is bending the law, such blatant reliance on trust could potentially negatively influence restaurants' motivation to comply with the guidelines. If some restaurants willingly want to misuse the system, this reliance on trust could very well be the most significant loophole in this whole regulatory compliance process. Therefore, having looked at the current practice, the author felt that there exists a clear need for automation in temperature measurement. The motivation for bending the rule may arise due to the availability of the opportunity of data mishandling and an automated temperature-measuring system replacing human involvement in scheduling and measuring the temperature would effectively remove this threat.

Moreover, the records look too easy to manipulate. Regardless of their form, paper-based or digital, the current practice relies on the trust that restaurants will not manipulate the records. However, if some restaurants to avoid hefty penalty try to manipulate the records, it would have been tough to identify; hence, there must have a method in place that assures recorded data is unaltered.

There also exists a grey area surrounding the accountability issue. In the event of having a breach of conduct, who should be held responsible looks complicated. It is easy for the quality controlling authority to issue a sanction against the restaurant, but that merely helps the company to solve the real problem, i.e. who should be held responsible? There are at least three entities who could play a role in a breach. The person: i) who schedules the reading, ii) who takes the reading and iii) who keeps the record of the reading. The author feels that it is necessary to reduce the accountability question to only one entity instead of having it floated over multiple places.

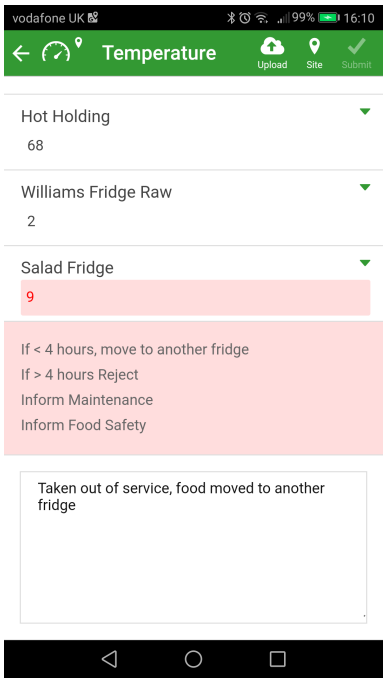

Figure 3: Screenshot of the smartphone application developed by Akeman Solutions who provide the service of keep record of data using digitised methods.

The current practice of recording temperature four times a day is also a weakness in the system. If the temperature moves over the threshold but returns to its normal state within six hours, it goes unnoticed. A continuation of such behaviour by a refrigerator potentially cause the health hazard, and it may go undetected for a long time. Thus, instead of four readings in 24 hours, the study proposes four readings every hour, i.e. keeping a record of the temperature every 15 min. This practice not only helps to detect unusual behaviour quickly but also creates scope for building smartphone applications using the temperature data to come up with additional notifications and machine learning-based analysis. Besides, due to the various size of the refrigerators, measuring temperature from a single location may not give the most appropriate reading always. By placing the IoT probes at different places in a small refrigerator, the study noticed that the temperature differs. This behaviour made the author suspect that for a large refrigerator, the difference could be significant.

4 REQUIRED TECHNOLOGIES

The Internet of Things and Blockchain are two disruptive technologies of the current time that shook the world with their potentials as soon as they arrive. Researchers around the world started talking about their impending success in a wide range of domains, including smart city, e-governance, finance, and so forth. However, as time passed by, those excellent ideas start to evaporate leaving doubts and disappointment behind. It took no time to raise questions about the effectivity and true potentials of these technologies. The lack of practical use-cases as to how these technologies can be utilised in the real-world scenario deepened the problem. Nevertheless, while investigating the regulatory compliance issues, the study found that these technologies are truly worthwhile in solving critical problems such as the one stated in this paper. Therefore, the followings briefly introduce these technologies and their key components in this section before using those in the proposed regulatory compliance model in the next section.

Internet of Things (IoT)

The Internet of Things (IoT) is sensing devices enabling many of the objects around us with the ability to communicate and transfer data. Depending on the working principle, the IoT can be of three types: internet-oriented that acts as middleware, things-oriented that provides with sensing ability and semantic-oriented that enables accessing knowledge [4]. A combination of these three types or just a standalone can be used to build smart applications aiming at solving critical problems in our daily life [6].

There are numerous methods available to enable devices with communication functionalities. One such method is to use Raspberry Pi with an appropriate sensor attached to it [9]. Such IoT device gives a considerable degree of freedom as it can easily be customised depending on the need of the application. Nevertheless, this flexibility comes with a cost. Each device requires lots of programming and configuration before it can be successfully deployed.

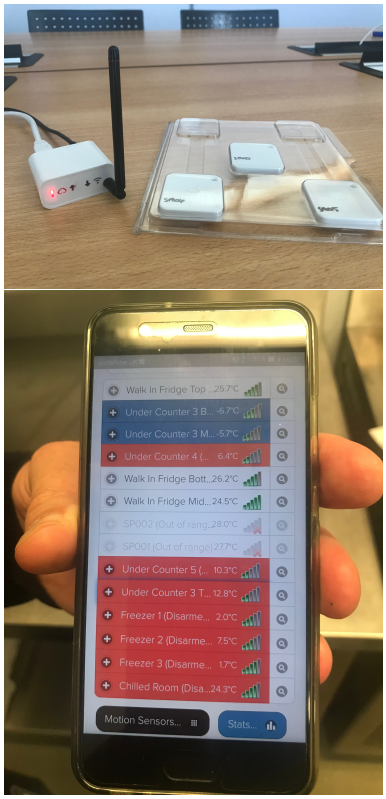

Figure 4: Above images show commercially available IoT devices and corresponding smartphone application to access the data quickly. The author used these sensors and the application to investigate the difference of temperature at the various locations of refrigerators; hence, emphasised on setting up one or more probes inside the same refrigerator depending on their size later in the proposed model.

On the other hand, commercially available IoT devices can also be used that allow less stress in setup and collecting data. However, most commercial device store data on their server, which could be a potential threat to privacy and security. While choosing IoT devices, use-case plays a vital role as the type heavily depends on the required services.

Blockchain

A Blockchain is an immutable public ledger for recording transactions [11]. Once inserted, a transaction becomes permanent and cannot be modified retroactively without the

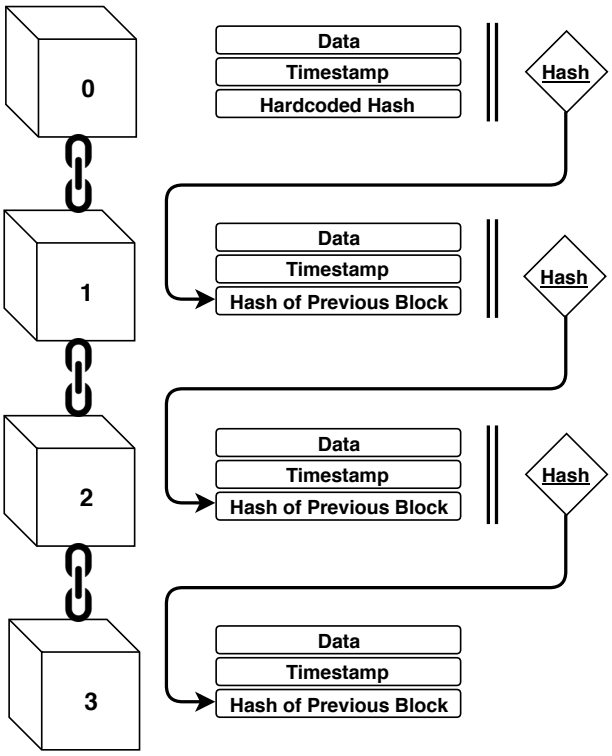

Figure 5: A high level overview of a Blockchain.

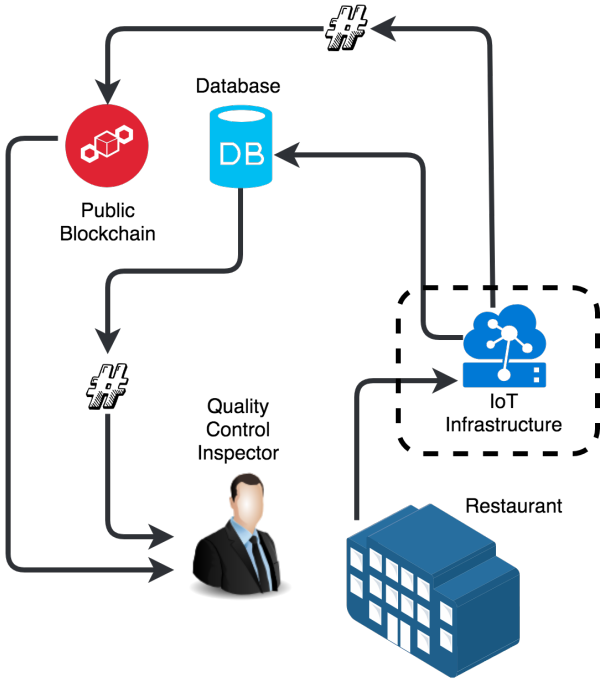

Figure 6: The proposed IoT and Blockchain-based regulatory compliance model.

alteration of all subsequent transactions, not even by the author. It is digitally constructed using a continuously growing list of records linked and secured by cryptographic principles, as shown in figure 5. Each of these records represents a block containing data, a timestamp and the cryptographic hash of the previous block. The insertion of the previous block's hash makes the blockchain resistant to modification of the data. Any attempt to alter a single block results in the collapse of the whole chain; hence, blockchain is considered immutable without the cooperation of the network majority.

Bitcoin was the first blockchain application that introduces this technology. Later many improved blockchains came into existence that not only removed the drawback of this pioneering application but also introduced new features. One of the most robust features is Smart Contract that allows writing Decentralised Applications (DApps) on the blockchain. Ethereum, EOS and NEO are few to name. These blockchains now allow us to connect IoT devices with the DApps and monitor data and trigger notifications if necessary [3]. A more detailed explanation of the blockchain technology can be found in the book *Inside Blockchain, Bitcoin, and Cryptocurrencies* [2].

5 PROPOSED REGULATORY COMPLIANCE MODEL

Figure 6 presents the proposed regulatory compliance model. The study considers IoT devices with temperature measuring capability in this model to replace human engagement in the day-to-day measurement process. Each refrigerator, depending on their size, should be assigned with one or more sensors to measure and send temperature data to a central server every 15-min using a secured IoT infrastructure. This data stays inside a secured database where host restaurant or bakery will have unrestricted access. The author recommends such custom because of two reasons: first, to enable restaurants using the data for improving quality of their services and second, they can make the data available to the third-party application developer to build smartphone and tablet-based applications. Keeping data inside a database also ensures restaurants' privacy because storing data directly inside a public Blockchain would make it open to the world.

That said, it is also essential to keep the data in a Blockchain to establish its unaltered status. Maintaining both privacy and immutability of data inside a public Blockchain is challenging because of the nature of this technology [13]. Public Blockchain is inherently open for all giving access to its data to anyone interested. On the other side, to protect the privacy of the restaurants, it must not be so open. Therefore, the author proposes the use of the cryptographic hash in this model

[8]. As shown in figure 6, automated and secured IoT devices create a hash of the entry it stores in the database and stores the hash instead of the original data in the Blockchain. This way, the system does not disclose the data but maintain its unaltered status. A food inspector can perform a hash operation on the database entry and match it with the Blockchain entry to get confirmation of the immutability of the data. If someone alters the data in the database, the corresponding hash entry will never match with the entry kept inside the Blockchain; hence, reveal the foul-play in the process.

One last problem of the system that the author was keen to address is the reduction of accountability in one place. The IoT infrastructure marked by the dashed box in figure 6 solves the issue of having accountability floated in three places mentioned earlier. Now we have it enclosed in one place. These devices need to be secured by design so that they cannot be tempered. Any attempt of temperament should hold the manager responsible; therefore, it will be his or her responsibility to make sure IoT infrastructure is operational, unbiased and unaltered.

6 CONCLUSION AND FUTURE STUDIES

The objective of this study was to present a theoretical model of regulatory compliance aiming at improving accountability for systems and data audit and introducing more transparency in management and quality control. The author took a field survey approach in this study to meet the restaurants' manager to understand the use-case involving temperature control under food safety compliance. Based on the author's experience and understanding, the study proposed that the IoT and Blockchain technology could potentially help the industry establishing more accountability and transparency in regulatory compliance. Next, with this research, the author has the plan to develop the model proposed in this paper and evaluate the performance in multiple restaurants as proof of concept.

ACKNOWLEDGEMENT

This work is fully funded by the Open University (OU) through the Strategic Data Science project. The author likes to thank the EU-funded CityLabs project for allowing to work with SMEs, particularly with the Akeman Solutions. Special thanks also go to Prof. Enrico Motta for his constant support and Mr Tim Butler for providing ideas and introducing the author of this work to the restaurants. The author also likes to thank the Open Blockchain group of the Knowledge Media Institute (KMi) of the OU for their suggestions, assistance and support.

REFERENCES

[1] Food Standards Agency. 2007. *Guidance on Temperature Control Legislation in the United Kingdom.* Technical Report. www.reading.ac.uk/foodlaw/pdf/uk-07039-temp-control-guidance.pdf

[2] N. Chowdhury. 2019. *Inside Blockchain, Bitcoin, and Cryptocurrencies.* Taylor & Francis.

[3] M. S. Ferdous, K. Biswas, M. J. Chowdhury, N. Chowdhury, and V. Muthukkumarasamy. 2019. *Advances in Computers.* Vol. 113. Elsevier, Chapter Integrated platforms for blockchain enablement. www.sciencedirect.com/science/article/pii/S0065245819300014

[4] J. Gubbia, R. Buyyab, S. Marusica, and M. Palaniswamia. 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems* 29, 7 (September 2013), pp 1645–1660. https://www.sciencedirect.com/science/article/pii/S0167739X13000241

[5] B. J. McCabe-Sellers and S. E. Beattie. 2004. Food safety: Emerging trends in foodborne illness surveillance and prevention. *Journal of the American Dietetic Association* 104, 11 (November 2004), pp 1708–1717. www.sciencedirect.com/science/article/pii/S0002822304014002

[6] J. Moore, G. Kortuem, A. Smith, N. Chowdhury, J. Cavero, and D. Gooch. 2016. DevOps for the Urban IoT. In *Proceedings of the Second International Conference on IoT in Urban Space.* Tokyo, Japan, pp 78–81. https://dl.acm.org/citation.cfm?id=2962747

[7] Government of the United Kingdom. 1995. *Food Safety (Temperature Control) Regulations 1995.* Technical Report. www.legislation.gov.uk/uksi/1995/2200/made

[8] B. Preneel. 1994. Cryptographic Hash Functions. *European Transactions on Telecommunications* (1994).

[9] M. Richardson and S. Wallace. 2012. *Getting started with raspberry PI.* O'Reilly.

[10] J. G. Sutinen and K. Kuperan. 1999. A socio-economic theory of regulatory complianceA socio-economic theory of regulatory compliance. *International Journal of Social Economics* 26, 1/2/3 (1999), pp 174–193. www.emerald.com/insight/content/doi/10.1108/03068299910229569/full/html

[11] M. Swan. 2015. *Blockchain: Blueprint for a new economy.* O'Reilly.

[12] Food Standard Agencies (UK). 2018. *How to chill, freeze and defrost food safely.* Technical Report. www.food.gov.uk/safety-hygiene/chilling

[13] G. Zyskind, O. Nathan, and A. S. Pentland. 2015. Decentralizing Privacy: Using Blockchain to Protect Personal Data. In *IEEE Security and Privacy Workshops.* San Jose, CA, USA.